529.346

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 April 2004 (15.04.2004)

PCT

(10) International Publication Number
WO 2004/032554 A1

(51) International Patent Classification[7]: H04Q 7/38

(21) International Application Number: PCT/IB2002/004031

(22) International Filing Date: 1 October 2002 (01.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **AHMAVAARA, Kalle** [FI/FI]; Hakaniemenranta 18 D 62, FIN-00530 Helsinki (FI). **HAVERINEN, Henry** [FI/FI]; Arkkitehdinkatu 15 A 3, FIN-33720 Tampere (FI).

(74) Agent: **UNGERER, Olaf**; Eisenführ, Speiser & Partner, Arnulfstr. 25, 80335 München (DE).

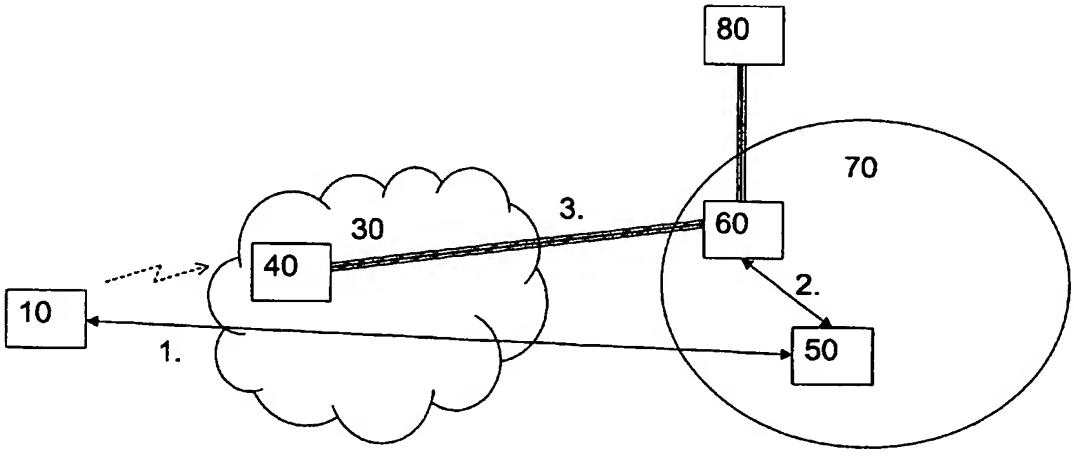
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR PROVIDING ACCESS VIA A FIRST NETWORK TO A SERVICE OF A SECOND NETWORK



(57) Abstract: The present invention relates to a method and system for providing access from a first network (30) to a service of a second network, wherein an authentication signaling is used to transfer a service selection information to the second network (70). Based on the service selection information, a connection can be established to access the desired service. Thereby, cellular packet-switched services can be accessed over networks which do not provide a context activation procedure or corresponding control plane signaling function.

WO 2004/032554 A1

Method and System for Providing Access via a First Network to a Service of a Second Network

FIELD OF THE INVENTION

The present invention relates to a method and system for providing access via a first network, for example a Wireless Local Area Network (WLAN), to a service of a second network, for example a service subscribed to in a General Packet Radio Service (GPRS) network or a Universal Mobile Telecommunications System (UMTS) network.

BACKGROUND OF THE INVENTION

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the earth. With tremendous success of wireless telephony and messaging services, it is hardly surprising that wireless communication is beginning to be applied to the realm of personal and business computing. No longer bound by the harnesses of wired networks, people will be able to access and share information on a global scale nearly anywhere they venture.

The major motivation and benefit from WLANs is increased mobility. Network users can move about almost without restriction and access LANs from nearly everywhere. In addition to increased mobility, WLANs offer increased flexibility. Meetings can be arranged, in which employees use small computers and wireless links to share and discuss future design plans and products. Such "ad hoc" networks can be brought up and torn down in a very short time as needed, either around the conference table and/or around the world. WLANs offer the connectivity and the convenience of wired LANs without the need for expensive wiring or re-wiring.

However, even with the fastest laptop, productivity while travelling can fall because of poor access to the Internet or company intranet. Despite the revolution of the Global System for Mobile communication (GSM), laptop users need faster access to download large files and to synchronize their e-mails quickly. The emerging mobile information society demands that data is available whenever and wherever. As a solution to this problem an operator WLAN solution has been proposed which brings broadband access to the laptop or terminal device in specific places like airports, convention centers, hotels and meeting rooms. Thus, mobile network op-

erators are able to offer broadband access to the internet, corporate intranets or other service machineries from virtually anywhere in the world. Thus, a public WLAN service with own WLAN roaming feature can be provided.

In packet-switched cellular networks, such as the GPRS or UMTS network, the users service descriptions are specified by Access Point Names (APN). GPRS is a common packet domain core network used for both GSM and UMTS networks. This common core network provides packet-switched services and is designed to support several quality of service levels in order to allow efficient transfer of non real-time traffic and real-time traffic. The Serving GPRS Support Node (SGSN) keeps track of the individual location of a mobile terminal and performs security functions and access control. The Gateway GPRS Support Node (GGSN) provides interworking with external packet-switched networks, and is connected with SGSNs via an IP-based packet domain backbone network. In the backbone network, the APN is in practice a reference to the GGSN to be used. In addition, the APN may, in the GGSN, identify the external network and optionally a service to be offered. Further details concerning the use and structure of APNs are defined e.g. in the 3GPP specification TS 23.003.

When a user connects to a GPRS service, i.e. establishes a Packet Data Protocol (PDP) context as specified e.g. in the 3GPP specifications TS 23.060, the APN information selected by the terminal device or user equipment (UE) or the user of the terminal device is sent from the terminal device to the network in a PDP context establishment signaling. This information consists of APN and optionally username and password if required to access the service behind the selected APN. In the GPRS network, this information is used to select suitable GGSN. The information also arrives to the selected GGSN and the GGSN uses this information further to establish a connection to a network node behind the GGSN, e.g. a corporate intranet or an operator service node. If provided, the username and password are delivered to the concerned network node behind the GGSN to allow authorization of the connection.

However, in the proposed public or operator WLAN systems, an operation similar to the GPRS PDP context activation is not provided. In particular, there is no dedicated signaling for setting up services between a WLAN terminal device, i.e. WLAN UE, and the WLAN network or network behind the WLAN network. Therefore, GPRS type of service selection and activation is not possible via the WLAN network, which thus forms a drawback in the proposed public or operator WLANs.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide a method and system for providing access from a WLAN network or any other first network to a service provided by a GPRS or any other second network.

This object is achieved by a method of providing access via a first network to a service facilitated by a second network, the method comprising the steps of:
- using an authentication message to signal a service selection information via said first network to an authentication server means of said second network; and
- using said service selection information to connect to services provided over an access point indicated by said service selection information.

Furthermore, the above object is achieved by an authentication server device for providing an authentication mechanism, said authentication being arranged:
- to extract from a received authentication message a service selection information for selecting a service; and
- to use said service selection information for establishing a connection to services provided over an access point indicated by said service selection information.

Additionally, the above object is achieved by a terminal device for providing access to a network service, said device being arranged to set in an authentication message a service selection information for selecting said network service.

Accordingly, a service selection information or service description is forwarded to the second network by using an authentication signaling between the terminal device and an authentication server of the second network, which then uses the service selection information to establish a connection to the desired or subscribed service. Thereby, access to network services of third parties is possible over the first network, e.g. the WLAN. Thus, dynamic service selection and multiple simultaneous connections to different services are enabled, and service continuity is obtained between different networks, such as WLANs and cellular packet-switched networks. Thereby, network flexibility and user mobility can be enhanced and service logics can be unified in different networks.

From the network operator's point of view, the proposed solution is advantageous in that current service description mechanisms, such as the APN mechanism in GPRS, can be used in new operator WLANs to thereby support legacy solutions.

The authentication message may be a message of the Extensible Authentication Protocol (EAP). In particular, the authentication message may be an EAP response message.

The service selection information may comprise at least one APN parameter. This at least one APN parameter may comprise an APN, a username and a password of the desired service. Furthermore, the APN parameter may be encrypted in the authentication message. The applied encryption for different APN parameters may be selected differently, so that selected APN parameters may be forwarded by the authentication server to the selected access point in encrypted format, and that the selected APN parameters are decrypted only at the access point or selected service network.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, the invention will be described in greater detail based on a preferred embodiment with reference to the accompanying drawings, in which:

Fig. 1 shows a schematic block diagram indicating the basic principles underlying the present invention;

Fig. 2 shows a schematic block diagram of a WLAN connected via a WLAN gateway of a GPRS network to an application server;

Fig. 3 shows an EAP signaling according the preferred embodiment of the present invention; and

Fig. 4 shows the format of an enhanced EAP Response Challenge packet according to the preferred embodiment.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The preferred embodiment will now be described on the basis of a network architecture as indicated in Figs. 1 and 2, where a WLAN user is authenticated to access a WLAN network by an EAP authentication to thereby get access to a cellular packet-switched service.

Fig. 1 shows a schematic block diagram of a network architecture comprising a WLAN 30 and a GPRS network 70. A terminal device or UE 10 which is subscribed to a GPRS service and wishes to get access to the service, first transfers a service selection information indicating at least one APN parameter and an optional username and password via the WLAN 30 to an authentication server 50 of the GPRS network 70 by using an authentication signaling, e.g. an authorisation request message (1st step). Then, the authentication server 50 selects a WLAN gateway 60 arranged in the GPRS network 70, signals the service information to the WLAN gateway 60, and as a response receives from the WLAN gateway 60 a connection information for establishing a connection between an access server 40 of the WLAN 30 and an application server 80 providing the requested service and being identified by the at least one APN parameter (2nd step). In particular, the authorisation request may be forwarded further to the application server 80 or another external AAA server together with the username and password and the WLAN gateway 60 first receives a response from there and then proxies this response to the access server 40.

Fig. 2 shows a more detailed block diagram of a network architecture in which the preferred embodiment of the present invention can be implemented. In Fig. 2, a WLAN UE 10 is connected via a wireless connection to an access point 20 of a WLAN 30. It is noted that the access point 20 has a similar functionality as a base station in a general cellular network. The access point 20 is not mobile and forms part of the wired network infrastructure. Further details regarding the architecture and function of the WLAN network 30 can be gathered e.g. from the IEEE specification 802.11.

Furthermore, the WLAN 30 comprises a WLAN access server 40 for establishing a connection to external networks such as a GPRS network 70 or another packet-switched network 90, e.g. the Internet or an operator or company intranet. The GPRS network 70 comprises an authentication server 50, , with an allocated authentication server database 55 in which subscriber information such as service profile information of each connected terminal device or UE are stored after retrieval of that information from a permanent subscriber database 110 at subscriber's home network 110. It is noted that the the functionality of the authentication server 50 can also be located at users home network or a WLAN backbone or subsystem. The authentication signaling with the UE 10 may be based on the EAP SIM authentication protocol in case a GSM SIM card is used within the UE 10. Alternatively, the authentication may be based on the EAP AKA (Authentica-

tion and Key Agreement) authentication protocol in case a UMTS SIM card is used within the UE 10.

The EAP protocol mechanism is used for authentication and session key distribution by means of the GSM SIM or the USIM. Authentication is based on a challenge-response mechanism, wherein the authentication algorithm which runs on the SIM or USIM card can be given a random number (RAND) as a challenge. The SIM or USIM runs an operator-specific confidential algorithm which takes the RAND and a secret key stored on the SIM or USIM as input, and produces a response (SRES) and a key as output. The key is originally intended to be used as an encryption key over the air interface. The authentication server 50 has an interface to the GSM or UMTS home network 100 of the UE 10 and operates as a gateway between the packet-switched AAA (Authentication, Authorization and Accounting) networks and the GSM or UMTS authentication infrastructure. After receiving an EAP identity response including user identification mappable to the user's International Mobile Subscriber Identity (IMSI) the authorization server 50 obtains n triplets or quintuplets from the authentication center at the home location register (HLR) or Home Subscriber Server (HSS) 110 of the user's home network 100. From the triplets, the authentication server 50 derives the keying material based on a cryptographic algorithm.

According to the preferred embodiment, the WLAN authentication signaling is used for signaling GPRS service subscription or selection information via the authentication server 50 to the GPRS network 70. The GPRS service information or service selection information comprises the APN of the desired service and an optional username and password required to connect to the service via the indicated APN. The authentication server 50 uses the obtained service selection information to select the WLAN gateway 60 having a similar function to a GGSN, from where the user can get access to the subscribed service. The subscribed service can be e.g. an access to a corporate intranet or to services of a mobile operator.

Fig. 3 shows a signaling diagram indicating an EAP-SIM authentication signaling between the UE 10 and the authentication server 50 of the GPRS network 70. The first EAP request (not shown) issued by the network is an EAP Identity Request. The client or UE 10 responds with an EAP Identity Response (step 1) comprising a pseudonym or IMSI. The pseudonym is used when an identity privacy support is being used by the UE 10. In response to the EAP Identity Response message or

packet, the authentication server 50 sends an EAP challenge request comprising the n random numbers RAND among other parameters (step 2). In response thereto, the UE 10 issues an EAP Challenge Response including the calculated response value SRES. Furthermore, according to the preferred embodiment of the present invention, the EAP Challenge Response also includes at least one encrypted APN parameter specifying the desired GPRS service to be accessed. The encrypted APN parameters my comprise the APN of the desired service and an optional username and password for getting access to the service (step 3). The applied encryption for different APN parameters may be selected differently. I.e., the APN itself may be the only APN parameter which is required for AP selection, and therefore only this parameter has to be in a format which is to be decrypted and/or read by the access server. The username and password parameters may be forwarded by the authentication server to the selected access point in encrypted format, and these parameters are decrypted only at the access point or selected service network. It is thus not possible to access them while transferred via the first network. If the authentication procedure was successful, the authentication server 50 responds with an EAP Success message (step 4).

The above authentication signaling procedure enables a signaling of service selection parameters to the authentication server 50 without requiring any additional context activation function as would be required in a conventional GPRS network without WLAN functionality. To achieve this enhanced functionality of the authentication signaling, the client software at the UE 10 is modified or programmed to add the respective service selection information to the EAP Challenge Response message. In particular, if a user has selected to connect to a specific service identified by its APN, the service information or service selection information is configured in the client software at the UE 10. For each service the following settings may be performed. Firstly, a free text entry identifying the service for the user may be set. Secondly, the APN, i.e. the identification of the Public Land Mobile Network (PLMN) plus the Domain Name Server (DNS) name assigned by the Mobile Operator (MO) may be set to point to the specific service, and, thirdly, a setting indicating whether the username and password are required (e.g. a Yes/No setting) can be made in the client software. The third setting may comprise a setting indicating either a predefined or a dynamic username or/and password setting.

At the latest after reception of the EAP request message, the UE 10 gets the required service selection related information from the user and encrypts it as specified by the utilised signalling protocol such as EAP-SIM. The UE 10 then inserts

the APN parameter information to the EAP Challenge Response message and sends it via the WLAN 30 to the authentication server 50.

Fig. 4 shows a format of the enhanced EAP SIM Challenge Response message according to the preferred embodiment as generated at the SIM. A "code" field is used to identify the message as a response message. An "identifier" field is one octet and aids in matching replies to responses. In particular, the "identifier" field must match the "identifier" field of the message to which it is sent in response. The "length" field indicates the length of the EAP message or packet. The "type" and "sub-type" fields are set to specific values specifying the EAP SIM Challenge Response message. The "reserved" fields are set to zero upon sending and ignored on reception. The "AT_SRES" field indicates an attribute value and is followed by an additional "length" field indicating the length of the following SRES value and by a "reserved" field. Finally, the proposed APN parameters specifying the requested service may be added e.g. as encrypted values.

It is noted that the present invention is not restricted to the described WLAN and GPRS service and can be used in any network architecture where a control plane signaling required for accessing a packet-switched service is not provided in the access network. The functionalities of the authentication server 50 and the gateway 60 not necessarily have to be GPRS functionalities, but can be located in any backbone network or subsystem of the WLAN or any other network accessible by the WLAN 30. They may be provided in standalone server devices or in GPRS GGSN or SGSN functionalities, respectively. Also, the accessed service does not have to be a GPRS service. Thus, the WLAN UE 10 can be a single-mode WLAN terminal without GPRS functionality but with a functionality to access external services via an authentication signaling, e.g. by a similar mechanism as the GPRS service selection mechanism. Furthermore, any given authentication message can be used for transferring the service selection information. The preferred embodiments may thus vary within the scope of the attached claims.

Claims

1. A method of providing access via a first network (30) to a service facilitated by a second network (90), said method comprising the steps of:
   a) using an authentication message to signal a service selection information via said first network to an authentication server means (50) of said second network (30); and
   b) using said service selection information to connect to services provided over an access point indicated by said service selection information.

2. A method according toclaim 1, wherein said first network is a wireless local area network (30).

3. A method according to any one of the preceding claims, wherein said second network is a cellular packet-switched network (70).

4. A method according to claim 3, wherein said cellular packet-switched network is a GPRS network (70).

5. A method according to any one of the preceding claims, wherein said authentication message is an EAP message.

6. A method according to claim 5, wherein said EAP message is an EAP SIM or EAP AKA message.

7. A method according to claim 5 or 6, wherein said authentication message is an EAP Challenge Response message.

8. A method according to any one of the preceding claims, wherein said service selection information comprises at least one APN parameter.

9. A method according to claim 8, wherein said at least one APN parameter comprises an APN, a username and a password.

10. A method according to claim 7 or 8, wherein said APN parameter is encrypted in said authentication message.

11. A method according to claim 9 or 10, wherein at least one of said APN parameters is encrypted so that it can only be decrypted at the network defined by the APN)

12. An authentication server device for providing an authentication mechanism, said authentication server (50) being arranged:
a) to extract from a received authentication message a service selection information for selecting a service; and
b) to use said service selection information for establishing a connection to services provided over an access point indicated by said service selection information.

13. An authentication server according to claim 12, wherein said authentication mechanism is based on an EAP protocol.

14. An authentication server according to claim 13, wherein said received authentication message is an EAP Challenge Response message.

15 15 An authentication server according to any one of claims 12 to 14, wherein said authentication server is a standalone WLAN authentication server (50).

16. An authentication server according to any one of claims 12 to 14, wherein said authentication server is a GGSN.

17. An authentication server device according to any one of claims 12 to 16, wherein said service selection information comprises at least one APN parameter.

18. An authentication server according to claim 17 , wherein said APN parameter is encrypted in said authentication message.

19. An authentication server according to claim 17 or 18, wherein at least one of said APN parameters is decrypted in said authentication server.

20. An authentication server according to claims 17 to 19 , wherein at least one of said APN parameter is forwarded by the authentication server to said access point in an encrypted manner.

21. A terminal device for providing access to a network service, said device being arranged to set in an authentication message a service selection information for selecting said network service.

22. A device according to claim 21, wherein said authentication message is an EAP message.

23. A device according to claim 22, wherein said EAP message is an EAP Challenge Response message.

24. A device according to claim 23, wherein said EAP Challenge Response message is an EAP SIM or EAP AKA Challenge Response message.

25. A device according to any one of claims 21 to 24, wherein said service selection information comprises at least one APN parameter.

26. A device according to any one of claims 21 to 25, wherein said service is a GPRS service.

27. A system for providing access from a first network (30) to a service of a second network (90), said system comprising a terminal device according to any one of claims 21 to 26, said terminal device (10) being connected to said first network (30), and an authentication server device (40) according to any one of claims 14 to 20, said authentication server being connected to said second network.

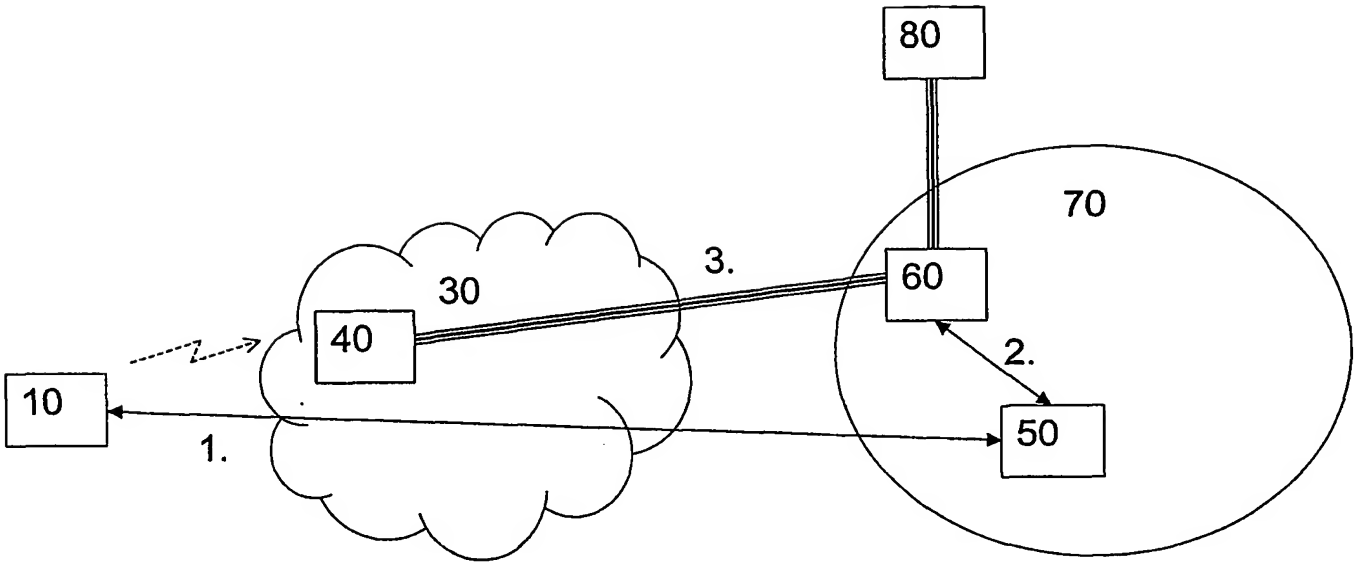


Fig. 1

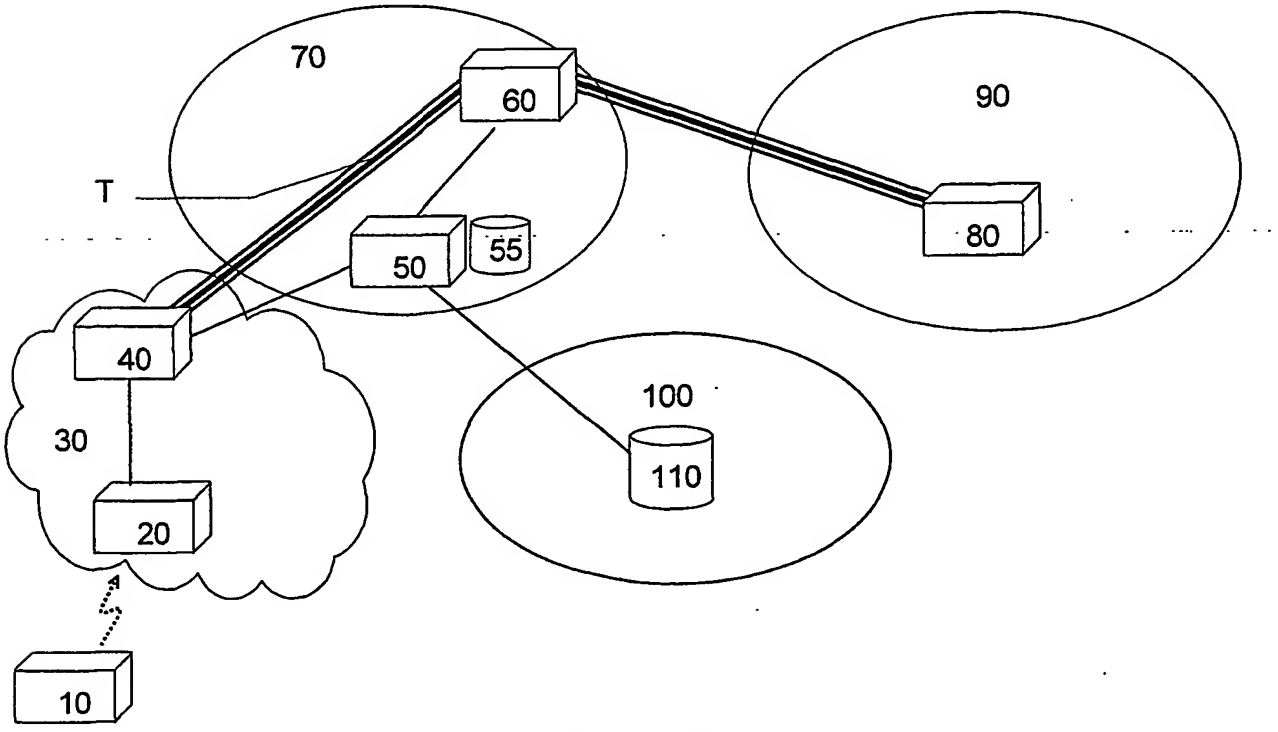


Fig. 2

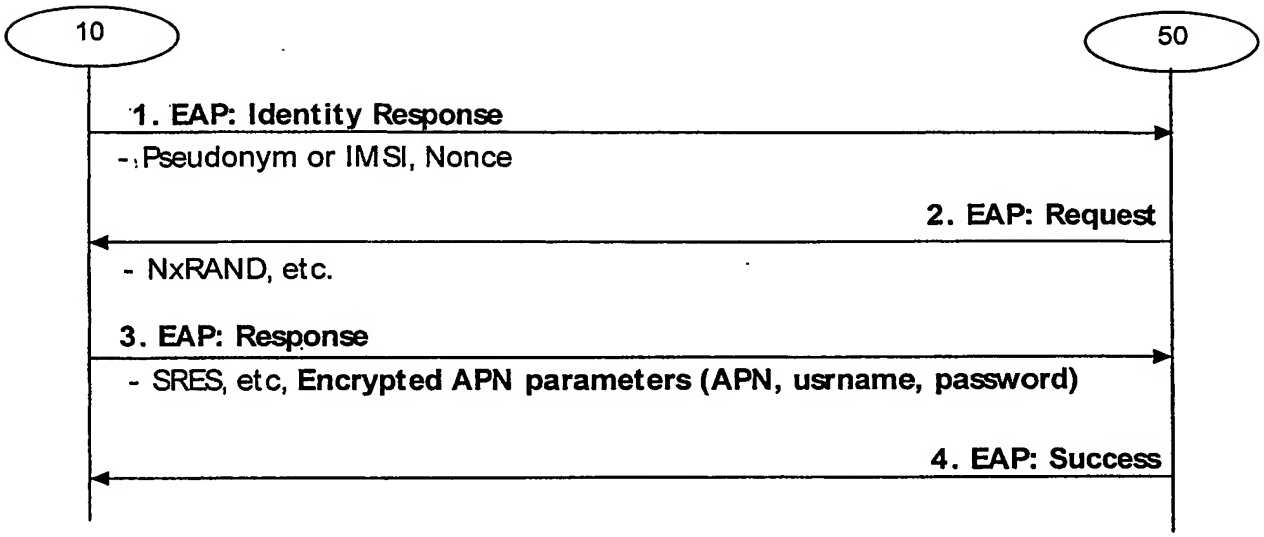


Fig. 3

Code	Identifier	Length
Type	Subtype	Reserved
AT_SRES	Length	Reserved
SRES		
APN parameter		

Fig. 4

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 02/04031

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 02 32084 A (HULKKONEN TONY ;HURTTA TUIJA (FI); NOKIA CORP (FI); THUOHINO MARKK) 18 April 2002 (2002-04-18) page 3, line 5 - line 19 page 6, line 20 -page 7, line 10 ---	1-4,12, 16,21, 26,27
A	WO 02 067617 A (BAECK JUHA ;HULKKONEN TONY (FI); NOKIA CORP (FI)) 29 August 2002 (2002-08-29) page 7, line 4 - line 18 abstract ---	1-27
A	US 2002/056001 A1 (YANG JIN ET AL) 9 May 2002 (2002-05-09) abstract; claims -----	1-27

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 May 2003	03. 06. 2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	STEFAN HANSSON/JA A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 02/04031

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0232084 A	18-04-2002	WO 0232170 A1	18-04-2002
		AU 1134801 A	22-04-2002
		AU 2060402 A	22-04-2002
		WO 0232084 A2	18-04-2002
WO 02067617 A	29-08-2002	WO 02067617 A1	29-08-2002
US 2002056001 A1	09-05-2002	AU 4327302 A	18-06-2002
		WO 0247350 A2	13-06-2002